AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Consultation response

Public Consultation on Guidelines 01/2025 on Pseudonymisation

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €3.7 trillion in 2022, directly supports more than 4.9 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

American Chamber of Commerce to the European Union
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 56, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

Executive Summary

The European Data Protection Board's (EDPB) Guidelines 01/2025 on Pseudonymisation address an important issue, offering organisations practical insights into the application of pseudonymisation[1] techniques under the General Data Protection Regulation (GDPR).

While the Guidelines contain useful clarifications, there remain several areas where adjustments could improve clarity, feasibility, and the promotion of innovation. In particular, the Guidelines should encourage the responsible use of pseudonymisation and privacy-enhancing technologies (PETs) while ensuring legal certainty and proportionality for businesses seeking to implement these tools.

Key recommendations

- Encourage the use of pseudonymisation and PETs. The Guidelines should actively promote these tools to support GDPR compliance while facilitating innovation.
- Adopt a proportionate approach to pseudonymisation. The protection afforded by pseudonymisation should reflect the sensitivity of the data and the context of its use – recognising the fact that pseudonymised data remains subject to the GDPR. Avoiding an unnecessarily high threshold and burdensome formalities will encourage its use by providing organisations with greater flexibility in its implementation.
- Clarify the concept of the 'pseudonymisation domain.' The definition should exclude unauthorised third parties and allow businesses to use legal and contractual safeguards to define access parameters.
- Reconsider the scope of 'additional information.' External data (such as publicly available sources) should not automatically be included in the definition, as this creates compliance challenges.
- Avoid imposing impractical obligations on businesses. The requirement for exporters to assess the capabilities of third-country security services is unrealistic and should be removed.
- Consider delaying the final Guidelines until the CJEU issues judgment in *SRB* (Case C-413/23 P) and the upcoming EDPB guidelines on anonymisation have been produced. This will help ensure the Guidelines provide a cohesive and stable analysis of pseudonymisation.

[1] The production of these Guidelines reflects the request in the Commission's Second Report on the application of the General Data Protection Regulation ("**Commission's Second GDPR Report**"), July 2024, at page 6

The Guidelines should encourage pseudonymisation and PETs

The GDPR is not a barrier to innovation

Sustainable competitiveness is a core goal for the EU in order to create a digital economy that is fair, competitive, facilitates groundbreaking research and creates a genuine single market for data.[2] The EU should strive to grow its economy and innovate in a way that respects fundamental rights but avoid excessive regulatory burdens (particularly for SMEs). This is especially important for the digital sectors, for which data is an essential tool, as evidenced by the EU wide range of initiatives in this area such as the adoption of the Data Governance Act, Data Act and European Health Data Spaces Regulation.[3]

The Guidelines therefore provide the EDPB with an opportunity to not only explain the concept to pseudonymisation but to **actively promote**[4] it as a practical and user-friendly tool for business and to demonstrate that the GDPR is not a barrier to innovation – ie show that the GDPR is "a legal framework that encourages responsible innovation".[5]

To do this, the Guidelines should be "*concise and practical [and] give answers to concrete problems and reflect a balance between data protection and other fundamental rights. [The] Guidelines should also be easy to understand for individuals without legal training, for example in SMEs*".[6]

A "gold-standard" will deter businesses from using pseudonymisation and other PETs

Businesses will consider three factors in mind when assessing pseudonymisation and other PETs:

1. What protection does the tool provide for personal data? Will it help demonstrate compliance with the GDPR?

2. What impact will that tool have on the usability of the data? In some cases, there is no reduction in utility. However, there is normally at least some impairment to its usefulness after the application of pseudonymisation and other PETs.

3. How difficult will it be to implement that tool to a standard that meets the relevant regulatory requirements, and to maintain that tool?

The decision to mandate a "gold-standard" in the Guidelines is concerning because of their focus on large-scale multi-party sharing of highly sensitive personal data. For example, there are multiple references to the need to conduct a risk analysis or assessment. A formal assessment, such as a Data Protection Impact Assessment (DPIA), will be important where the underlying data poses significant risks because of its sensitivity or scale, or the context in which it is used. However, a formal assessment

[2] See the Commission's Second GDPR Report, and the *Draghi Report, The future of European competitiveness*, September 2024.

[3] See the Commission's Second GDPR Report at page 16.

[4] In particular, the intent of the GDPR is to incentivise pseudonymisation as per recital 29.

[5] As per the *EDPB Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*, 17 December 2024

[6] See the Commission's Second GDPR Report at page 6.

may not be appropriate for low risk use cases, such as where it pseudonymisation is used as an additional protective measure for low risk data shared on an intra-group basis.

The Guidelines therefore risk deterring, rather than encouraging, the take up of pseudonymisation. Put differently, many businesses (particularly SMEs) will just see pseudonymisation as a difficult and technical concept that is out of their reach.

This is a missed opportunity. The EDPS should be encouraging businesses to deploy pseudonymisation and similar PETs in a wide range of situations. The EDPS should moderate the tone of the Guidelines to make it clear pseudonymisation is a practical user-friendly tool that can be applied flexibly according to the sensitivity of the underlying personal data - in other words, in line with the GDPR's risk-based approach, pseudonymisation is a means to ensure "*low-risk processing activities do not bear a substantial compliance burden*".[7] Some suggestions to achieve this can be found below.

Finally, the Guidelines are also an opportunity to promote other PETs more widely. For example, the Guidelines might explore the potential to combine pseudonymisation with PETs to strengthen the protection of personal data and special category data. The Guidelines could also explore how pseudonymisation can be applied in unstructured data.

Concepts, such as “pseudonymisation domain”, are generally helpful

Pseudonymisation domain as an optional framework for assessment

Introducing the concept of the “pseudonymisation domain” as an optional framework for controllers to assess the effectiveness of a pseudonymisation solution is a positive addition.

In particular, the ability of controllers to impose controls over the flow of information, and thus create a bespoke “pseudonymisation domain” (see paragraph 35) means this concept can be applied in a wide range of potential solutions. The requirement to define the objectives of pseudonymisation, establish the domain, choose the technical and organisational measures and means of attribution, also provide a sound methodology to protect personal data (see paragraph 94).

However, there must be sensible boundaries to the “pseudonymisation domain”. For example, there is a suggestion that the pseudonymisation domain might include unlawful recipients of the data, which presumably might include cyber criminals (see paragraph 37). This should be dealt with as a security issue under Article 32, GDPR. The controller is simply unable to identify at the outset all persons who are not legitimate recipients of the pseudonymised data but “*may attempt to gain access to it anyway*”. Having to include such malicious actors or unauthorised recipients in the “pseudonymisation domain” makes the concept unworkable for most use cases.

It would also be helpful to clarify that appropriate and binding technical, contractual, organisational or policy arrangements can be used to delineate the “pseudonymisation domain” and, in paragraph 38 of the Guidelines, that the pseudonymisation domain could consist of a separate group company – ie that the “single recipient” could be a company within a wider group.

[7] *Ibid*.

Finally, the confirmation that it is possible to use a consistent identifier for a data subject within the "pseudonymisation domain" whilst still treating that data as pseudonymised is a positive step (eg paragraph 99) that is critical to the operation of pseudonymisation.

Additional information should not include external information

The concept of "additional information" needs to be more strictly defined. It should be limited to:

- *Original data*: Data before the pseudonymising transformation
- *Pseudonymisation secrets*: This is information such as the encryption key or look-up table

It is problematic to extend the definition of "additional information" to other data sources, such as public data or social media posts (as per paragraph 21). It is very hard to reconcile this broad definition with, for example, the obligation in paragraph 66: "*all entities holding additional information should provide sufficient guarantees to the exporter*". It would not be possible for the exporter to obtain any sort of guarantee from innumerable holders of external public information.

The attribution analysis should include external information (to the extent that is accessible within "means reasonably likely to be used" by the relevant entity) but should not form part of the "additional information".

Frameworks not legal concepts

As set out above, the Guidelines' new concepts like "pseudonymisation domain", "pseudonymisation secrets" and "quasi-identifiers" are generally positive. However, the Guidelines should emphasise that they are not legal concepts as such and instead simply a framework that controllers may wish to adopt to assess any pseudonymisation solution. They should not be mandatory and should not create any new obligations or have any direct legal bearing.

"Attribution" test should reflect the sensitivity of the data

Sensitivity and scale are important

The approach to "attribution" and the requirements for the pseudonymisation solution, should reflect:

- *The sensitivity of the underlying data*: Clearly special category data, such as medical information, will need a high degree of protection. In contrast, less sensitive data (such as public data or technical data) may warrant a more flexible approach.
- *The scale of the processing*: Again, where a processing affects a very large number of data subjects, greater protection will be needed. Small populations may, depending on the circumstances, create less risks.
- *The number of parties involved*: Where the data is to be shared between a number of different parties, more sophisticated solutions may be needed such as a Trust Centre; but they are

hardly likely to be needed for intragroup sharing where there should be more flexibility as to the means used to prevent attribution.

- *The potential motivations of any intruder*: This largely ties back to the sensitivity of the underlying data but in a situation in which there is limited or no real incentive to access the data, the requirements for the solution should be more flexible.

The current Guidelines appear to be squarely aimed at situations in which very large amounts of highly sensitive personal data are processed, often in a multiparty scenario. For example, six of the examples relate to medical information or other special category personal data.

This approach appears to influence some of the expectations/recommendations for pseudonymisation, such as: (a) prescriptive requirements for encryption, including cipher text indistinguishability (para 106); (b) only using vetted and specially trained personnel to implement the pseudonymisation (para 109); and (c) daily key rotation (para 115). Furthermore, the absolute criteria presented in paragraph 47, such as requiring that third parties be "not able to reconstitute" the original data, are inconsistent with the "reasonably likely" standard and the flexible nature of pseudonymised data.

Comments on the Guidelines' examples

This impression of a "gold standard" also traces through to the examples given in the Guidelines. Some relate to large-scale, multiparty sharing of highly sensitive medical data, where a "gold-standard" is appropriate. However, even in the other examples the approach taken appears to be disproportionate:

Example 8 - Purchase histories from a web-shop

The analysis of purchases from an e-commerce platform to determine purchasing patterns is a well-established activity that would be well within most customer's expectations.

Pseudonymising direct identifiers for the purpose of the analysis is good practice. However, this example should really recognise that the underlying data is unlikely to be sensitive and the 'Team of Analysts' has no obvious motive to identify the customers. On that basis, it could explore the use of legal or contractual controls as a substitute to strict application of pseudonymisation (such as sifting through the order details to try to remove any "individualised entries") particularly given the customer data remains subject to the GDPR at all times.

Many projects would benefit from a simple pseudonymisation solution based on encryption of direct identifiers but are much less likely to adopt a significantly more complex solution that requires them to develop, test and maintain complex technology to identify and remove identifiers from unstructured data.

Example 9 – Employee satisfaction survey

This example considers the position of an employee satisfaction survey stored by a service provider in a third country that does not meet the European Essential Guarantees. It describes a series of sophisticated technical steps to protect that information in case the information is obtained by the authorities of the third country.

Again, the starting point should be an assessment of scale, sensitivity and motivations. Law enforcement and security authorities (regardless of their location) do not have unlimited resources. Quite apart from any legal constraints, those authorities will focus those resources on issues of national security (such as terrorism) or serious crime, and will focus on risks in their own jurisdiction. It seems unlikely that those authorities would expend valuable resources to find out if a group of employees working for a company in another country are happy in their jobs.

The GDPR allows for "degrees" of pseudonymisation

The approach described above is also driven by the proper interpretation of Article 4(5) of the GDPR – ie whether the data can "*no longer be attributed to a specific data subject*". To achieve this there must be "*technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*".

This "attribution" test is different and much less strict than the test of whether information is personal data. This is for two reasons as described below.

If a very strict approach is applied in practice, the information will most often fall outside the GDPR altogether

The Guidelines appear to apply a very high test for effective pseudonymisation. In some cases, it seems to be tantamount to asking if the receiving entity has no "*means reasonably likely to be used*" to reidentify the individual.

However, if this test is applied in practice, it makes the concept of "pseudonymisation" largely redundant as in many cases the information will not be personal data in the first place and the GDPR does not apply (see *Breyer* and *Scania*).[8]

In addition, the approach in the Guidelines to the concept of personal data is inconsistent with those cases. For example, at paragraph 22 the Guidelines state that "*Pseudonymised data, which could be attributed to a natural person by the use of additional information, is to be considered information on an identifiable natural person, and is therefore personal. This statement also holds true if pseudonymised data and additional information are not in the hands of the same person*". This appears to be inconsistent with the Advocate General's opinion in SRB C-413/23 P.

There are good policy reasons to recognise "degrees" of pseudonymisation

[8] Albeit there may still be GDPR obligations on the disclosing entity, as per SRB.

More importantly, pseudonymised data continues to be personal data and so subject to the GDPR.[9] This is not a concept that takes the information outside of the scope of the GDPR; but rather one that can help demonstrate various aspects of the GDPR such as data protection by design or data security.

Accordingly, while there is a binary distinction between information being personal data (or not) there is no conceptual or practical problem in recognising "degrees" of pseudonymisation. In other words, the Guidelines should acknowledge the possibility for the strength of pseudonymisation to vary - albeit the less strong the pseudonymisation, the less effective it will be to demonstrate compliance with data protection by design, data security etc.

This is supported by the wording of the GDPR, particularly Article 4(5) which confirms that technical or organisational means can be used to protect the additional information in order that the personal data "*are not attributed*" to an individual; not "*cannot be*" attributed.

Improvements to the "attribution" test

It would be helpful for the Guidelines to: (a) state that that the test is not the same as that for determining if information is personal data; and (b) recognise pseudonymisation is a broader concept. This would incentivise business to use pseudonymisation flexibility, without in any way undermining the protection of that personal data.

Finally, given the strong overlap between these Guidelines and: (a) the upcoming EDPB guidelines on anonymisation; and (b) the CJEU's decision in *SRB*, these Guidelines should be delayed until both are finalised. Adopting the guidance on pseudonymisation and anonymisation in parallel will help ensure that the Guidelines provide a cohesive and stable analysis given the relationship between these two similar, but very different, concepts.

Other comments

Data subject rights

The EDPB should take two comments into consideration regarding its suggestion that controllers should tell the data subjects how they can obtain the pseudonyms relating to them, and how they can be used to demonstrate their identity.

Firstly, there is a suggestion that a controller should inform data subjects that it holds pseudonymised data "if possible" (end of paragraph 77). This is confusing and seems to go against the logic of Article 11(1), which exists to reduce burdens when identifiability is not reasonably possible, not to create new ones. It is unclear how this is intended to apply in light of Article 14(5) and seems to undermine the benefits of using pseudonymisation. This should be removed or at least clarified.

[9] Recitals 26 and 28.

Second, the Guidelines suggest an entirely new obligation to tell data subjects how to "*obtain the pseudonyms relating to them, and how they can be used to demonstrate their identity*". It is not clear what the legal basis for this obligation is and seems to go well beyond the requirements of Article 13-15 of the GDPR and is generally unhelpful. There should be minimal privacy risk from this information and these disclosures will make privacy notices even longer and less likely to be read by data subjects.[10] This is a further deterrent to the use of pseudonymisation.

Assessment of the capabilities of third country authorities

The Guidelines suggest that, in the context of transfers to third countries, exporters should assess the information available to third country authorities, including its security services. The operational capabilities of the security services (both in the EU and in third countries) are closely guarded secrets.

Many businesses are grappling with the need to assess third country laws under *Schrems II*. This is an extremely burdensome and expensive process and outside of the resources of many large businesses (let alone SMEs).

However, the requirements of the Guidelines go a stage further and are simply impossible for any exporter. There is no practical means for exporters to get accurate and comprehensive information about the capabilities of third country authorities, including its security services. This obligation should be removed from the Guidelines.

Personal data breaches

The Guidelines suggest that any situation in which there is unauthorised reversal of pseudonymisation is a personal data breach and may require notification to the relevant supervisory authority (paragraph 80). In practice, pseudonymisation is a technology that should be capable of use in a wide variety of situations, including where the level of risk is low regardless of whether or not the pseudonymisation process is reversed (see the comments on Example 8 above) so it would be helpful to qualify this statement.

[10] *No One Reads Privacy Notices. So Why Do We Have Them?* Global Privacy Law Review, Volume 5, Issue 4, Nov 2024 but noting the CJEU may address this *SRB*.